FORM-PTO-1390 (Rev. 12-29-99)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 032326-135

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5): Unassigned 09/830206

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR99/02233	21 September 1999	27 October 1998

TITLE OF INVENTION: Method and System for Authenticating Users and Managing Risk in a Communication Network (AS AMENDED)

APPLICANT(S) FOR DO/EO/US: Jean-Pierre LE GALL and Gary CHEW

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

JC18 Rec'd PCT/PTO 2 4 APR 2001

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
Unassigned 09/830206	PCT/FR99/02233	032326-135

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1,000.00 (960)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $860.00 (970)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $710.00 (958)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) $690.00 (956)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00 (962)		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(e)).	$ -0-	

Claims	Number Filed	Number Extra	Rate		
Total Claims	4 -20 =	-0-	X$18.00 (966)	$ -0-	
Independent Claims	1 -3 =	-0-	X$80.00 (964)	$ -0-	
Multiple dependent claim(s) (if applicable)			+$270.00 (968)	$ -0-	
			TOTAL OF ABOVE CALCULATIONS =	$ 860.00	
Reduction for 1/2 for filing by small entity, if applicable (see below).				$ -0-	-
			SUBTOTAL =	$ 860.00	
Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(f)). +				$ -0-	
			TOTAL NATIONAL FEE =	$ -0-	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property +				$ -0-	
			TOTAL FEES ENCLOSED =	$ 860.00	
			Amount to be: refunded		$
			charged		$

a. ☐ Small entity status is hereby claimed.

b. ☒ A check in the amount of $ 860.00 to cover the above fees is enclosed.

c. ☐ Please charge my Deposit Account No. 02-4800 in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

d. ☐ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

SIGNATURE

James A. LaBarre
NAME

28,632
REGISTRATION NUMBER

(01/01)

Patent
Attorney's Docket No. 032326-135

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Jean-Pierre LE GALL et al	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: April 24, 2001	)	
	)	
For: METHOD AND SYSTEM FOR AUTHENTICATING USERS AND MANAGING RISK IN A COMMUNICATION NETWORK (AS AMENDED)	)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

IN THE TITLE:

Replace the original title with the following:

--METHOD AND SYSTEM FOR AUTHENTICATING USERS AND MANAGING RISK IN A COMMUNICATION NETWORK--

IN THE SPECIFICATION:

Page 1, immediately following the title appearing on lines 1 and 2, insert the following:

--This disclosure is based upon, and claims priority from French Application No. 98/13440, filed on October 27, 1998 and International Application No. PCT/FR99/02233, filed September 21, 1999, which was published on May 4, 2000 in a language other than English, the contents of which are incorporated herein by reference.

Background of the Invention--

Page 3, between lines 20 and 21, insert the following heading:

--**Summary of the Invention** --.

Page 6, immediately before the first paragraph, insert the following heading:

--**Brief Description of the Drawings**--.

Page 6, between lines 14 and 15, insert the following heading:

--**Detailed Description**--.

IN THE CLAIMS:

Kindly replace claims 1-4, as follows.

1. (Amended) A risk management system in a communication network of a type which includes a message service and communication devices each having an

electronic chip card capable of calculating a cryptographic authentication certificate from a value supplied by the network, comprising:

means in said chip cards for selectively enabling the calculation of a cryptographic certificate and its transmission to the network when certain conditions are fulfilled, and for transmitting to the network a message requesting evaluation of risk when other conditions are fulfilled, and

means in said network for evaluating said risk according to the information contained in the risk evaluation request message and parameters specific to the user of the communication devices, and for sending a message to said enabling means in the electronic chip card for enabling or inhibiting the calculation and transmission of the cryptographic certificate.

2. (Amended) A risk management system according to Claim 1, wherein said electronic chip card, executes the following steps:

(a) checking whether the electronic chip card is in an inhibited state in order to determine whether to refuse an authentication request;

(b) in the case of authorisation of the authentication request, counting the number (N) of requests for authentication of the electronic chip card by the network,

(c) comparing the number (N) of authentication requests with a first threshold T0,

(d) calculating a cryptographic certificate if $N < T0$ and transmitting it to the network,

(e) comparing the number N with a second threshold T1 if $N \geq T0$,

(f) putting the electronic chip card in the inhibited state if $N \geq T1$, and

(g) calculating a cryptographic certificate and producing a risk assessment request message, and transmitting said certificate and message to the network if $T0 < N \leq T1$.

3. (Amended) A system according to Claim 2, wherein the network executes the following steps:

(h) analysing the risk assessment request transmitted by the electronic chip card,

(i) assessing the risk according to the results of the analysis according to the previous step (h) and parameters specific to the user of the communication device, and

(j) producing a response message and transmitting it to the electronic chip card.

4. (Amended) A system according to claim 3, wherein the numbers N, T0 and T1 are monetary values corresponding respectively to a totalling of the expenditure made in communications sessions, a first authorised expenditure threshold and a second threshold beyond which the expenditure is no longer authorised.

Add the following new claims:

--5. A system according to claim 2, wherein the numbers N, T0 and T1 are monetary values corresponding respectively to a totalling of the expenditure made in communications sessions, a first authorised expenditure threshold and a second threshold beyond which the expenditure is no longer authorised.

6. A method for managing authenticating users and managing risks in a communication network of a type having a message service and communication devices with electronic chip cards that authenticate said devices to the network, comprising the following steps performed in the chip card:

(a) checking whether the electronic chip card is in an inhibited state in order to determine whether to refuse an authentication request;

(b) in the case of authorisation of the authentication request, counting the number (N) of requests for authentication of the electronic chip card by the network,

(c) comparing the number (N) of authentication requests with a first threshold T0,

(d) calculating a cryptographic certificate if $N < T0$ and transmitting it to the network,

(e) comparing the number N with a second threshold T1 if $N \geq T0$,

(f) putting the electronic chip card in the inhibited state if $N \geq T1$, and

(g) calculating a cryptographic certificate and producing a risk assessment request message, and transmitting said certificate and message to the network if $T0 < N \leq T1$.

7. The method of claim 6 wherein the network executes the following steps:

(h) analysing the risk assessment request transmitted by the electronic chip card,

(i) assessing the risk according to the results of the analysis according to the previous step (h) and parameters specific to the user of the communication device, and

(j) producing a response message and transmitting it to the electronic chip card.

8. The method of claim 7 wherein the numbers N, T0 and T1 are monetary values corresponding respectively to a totalling of the expenditure made in communications sessions, a first authorised expenditure threshold and a second threshold beyond which the expenditure is no longer authorised.

9. The method of claim 6 wherein the numbers N, T0 and T1 are monetary values corresponding respectively to a totalling of the expenditure made in communications sessions, a first authorised expenditure threshold and a second threshold beyond which the expenditure is no longer authorised.--

REMARKS

Entry of the foregoing amendment is respectfully requested. This amendment is intended to place the claims in a more conventional format and eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: April 24, 2001

Attachment to Preliminary Amendment dated April 24, 2001

Marked-up Claims 1-4

1. (Amended) A risk management system in a [mobile telephony] communication network [equipped with a message service device (18), the mobile handsets (14) each having] of a type which includes a message service and communication devices each having an electronic chip card [(22) (SIM)] capable of calculating a cryptographic authentication certificate from a value supplied by the network, [characterised] comprising:

[- in that the electronic chip card (22, SIM) comprises means (32)] means in said chip cards for selectively enabling [or not] the calculation of a cryptographic certificate and its transmission [(56)] to the network when certain conditions are fulfilled, [or not] and for transmitting to the network a message [(38)] requesting evaluation of [the] risk when other conditions are fulfilled, and

[- in that the network (54) comprises means (34)] means in said network for evaluating [the] said risk according to the information contained in the risk evaluation request message [(38)] and parameters specific to the user of the [mobile handset (14, ME)] communication devices, and for sending a message [(40) to the said means (32) of] to said enabling means in the electronic chip card for enabling or [not] inhibiting the calculation and transmission of the cryptographic certificate.

2. (Amended) A [method for implementing the] risk management system according to Claim 1, [characterised in that it comprises, in the] wherein said electronic chip card [(22)], executes the following steps [consisting in]:

Attachment to Preliminary Amendment dated April 24, 2001

Marked-up Claims 1-4

(a) checking [(74) the state, inhibited or not, of] whether the electronic chip card is in an inhibited state in order to determine whether to refuse [(75) or not the] an authentication request;

(b) in the case of authorisation of the authentication request, counting [(76)] the number (N) of requests for authentication of the electronic chip card [(22, SIM)] by the network [(54)],

(c) comparing the number (N) of authentication requests with a first threshold T0,

(d) calculating a cryptographic certificate if $N < T0$ and transmitting it to the network,

(e) comparing the number N with a second threshold T1 if $N \geq T0$,

(f) putting the electronic chip card [(22, SIM)] in the inhibited state [(82, 58)] if $N \geq T1$, and

(g) calculating a cryptographic certificate [(88)] and producing a risk assessment request message, [(86)] and transmitting [(38, 56) them] said certificate and message to the network if $T0 < N \leq T1$.

3. (Amended) A [method] system according to Claim 2, [characterised in that it also comprises the following steps implemented by] wherein the network [(54), consisting in] executes the following steps:

Attachment to Preliminary Amendment dated April 24, 2001

Marked-up Claims 1-4

(h) analysing [(94)] the risk assessment request transmitted by the electronic chip card [(22)],

(i) assessing [(96, 102, 98)] the risk according to the results of the analysis according to the previous step (h) and parameters specific to the user of the [mobile handset] communication device, and

(j) producing [(100, 104, 40)] a response message and transmitting it to the electronic chip card [(22)].

4. (Amended) A [method] system according to [one of the preceding Claims 2 or 3, characterised in that] claim 3, wherein the numbers N, T0 and T1 are monetary values corresponding respectively to a totalling of the expenditure made in [telephone] communications sessions, a first authorised expenditure threshold and a second threshold beyond which the expenditure is no longer authorised.

A RISK MANAGEMENT METHOD AND SYSTEM IN A MOBILE TELEPHONY NETWORK

The invention relates to mobile telephony networks and more particularly, in such networks, a method and a system for managing the risk incurred by the operator of the mobile telephony network vis-à-vis users liable to exceed their rights or abnormal operations.

A mobile telephony system of the GSM (the acronym of the English expression Global System for Mobile communications) type, comprises a mobile telephony network, managed by an operator, which makes it possible to connect together users each provided with a mobile handset ME (the acronym of the English expression "Mobile Equipment"), each handset comprising notably an electronic chip card SIM (the acronym of the English expression "Subscriber Identification Module").

In such a mobile telephony system, a certain number of operations are provided for the

authentication of the SIM card by the network, at the time the handset is switched on, and at any other time in the telephone communication.

To this end, the authentication method comprises the following steps consisting in:

(1) the resetting of the card by the handset or mobile equipment ME and the transmission of the identity of the SIM card to the network,

(2) obtaining from the network a random number RN at the request of the handset ME,

(3) transmitting the random number RN to the SIM card by means of the handset ME,

(4) calculating in the SIM card a first cryptographic certificate CC1 or cryptogram according to a predefined algorithm AL, using the random number RN supplied by the network and a secret key SC internal to the SIM card,

(5) transmitting to the network, via the handset ME, the first cryptographic certificate CC1 calculated by the SIM card,

(6) calculating a second cryptographic certificate CC2 by means of the network according to the same algorithm AL as that of the SIM card, using the random number RN sent to the SIM card and the secret internal key SC which is known to the network through the identity of the SIM card,

(7) comparing the second cryptographic certificate CC2 with the first cryptographic certificate CC1, and

(8) enabling the transaction if the comparison is positive or inhibiting it in the contrary case.

Such an authentication method makes it possible to verify that the bearer of the handset ME with which the SIM card is associated is indeed authorised to enter into communication by means of the network. However, this method does not make it possible to take into account other conditions which would have to be fulfilled in order to enable the establishment of communication. One of the additional conditions to be fulfilled could, in the case of a prepayment card, be that the amount remaining to the credit of the bearer of the handset is greater than a certain predetermined threshold, this condition tending to limit the risk of any payment default.

Moreover, the authentication methods currently implemented do not make it possible to detect repeated access requests by a fraudster using a stolen handset and, all the more so, blocking this access after a certain number of access requests.

One aim of the present invention is therefore to implement a method of authenticating a subscriber card for a telecommunications network which makes it possible to take into account different conditions, possibly liable to change, so as to manage or limit the risks incurred by the operator by authorising access to the network.

This aim is achieved by introducing means into the SIM card of the handset and into the network server; these means communicate with each other by means of

messages transmitted over a service telecommunication channel such as the one currently used for the short messages service better known by the English acronym SMS, standing for "Short Message Service".

The invention therefore relates to a risk management system in a mobile telephony network equipped with a message service device, the mobile handsets each having an electronic chip card SIM capable of calculating a cryptographic authentication certificate from a value supplied by the network, characterised:

- in that the electronic chip card comprises means for enabling or not the calculation of a cryptographic certificate and its transmission to the network when certain conditions are fulfilled or not and for transmitting to the network a message requesting evaluation of the risk when other conditions are fulfilled, and

- in that the network comprises means for evaluating the said risk according to the information contained in the risk evaluation request message and parameters specific to the user of the mobile handset and for sending a message to the said means of the electronic chip card for enabling or not the calculation and transmission of the cryptographic certificate.

The invention also relates to a method for implementing the risk management system defined above, characterised in that it comprises, in the electronic chip card, the following steps consisting in:

(a) checking the state, inhibited or not, of the electronic chip card in order to refuse or not the authentication request;

(b) in the case of authorisation of the authentication request, counting the number N of requests for authentication of the electronic chip card by the network,

(c) comparing the number N of authentication requests with a first threshold T0,

(d) calculating a cryptographic certificate if $N < T0$ and transmitting it to the network,

(e) comparing the number N with a second threshold T1 if $N \geq T0$,

(f) putting the electronic chip card in the inhibited state if $N \geq T1$, and

(g) calculating a cryptographic certificate and producing a risk assessment request message and transmitting them to the network if $T0 < N \leq T1$.

The above method is characterised in that, in the network, it comprises the following additional steps consisting in:

(h) analysing the risk assessment request transmitted by the electronic chip card,

(i) assessing the risk according to the results of the analysis according to the previous step (h) and parameters specific to the user of the mobile handset, and

(j) producing a response message and transmitting it to the electronic chip card.

Other characteristics and advantages of the present invention will emerge from a reading of the following description of a particular example embodiment, the said description being given in relation to the accompanying drawings, in which:

- Figure 1 is a diagram showing schematically the information flows between the different components of the mobile telephony network,

- Figure 2 is a functional diagram of a risk management module associated with the electronic chip card of a mobile handset, and

- Figure 3 is a functional diagram of a risk management module associated with the mobile telephony network.

A mobile telephony network comprises schematically three parts A, B and C which are delimited vertically by two dotted lines 10 and 12.

The central part B corresponds to the bilateral radio transmission of the communications, between a mobile handset 14 (or ME) and a base station 16 (or BS, corresponding to the acronym of the English expression "base station") associated with messaging equipment 18 (or SMSC, corresponding to the acronym of the English expression "Short Message Service Centre"), which supplies the SMS (the acronym of the English expression "Short Message Service") defined above in the introduction.

The part C corresponds to the mobile telephony network 54 and comprises notably a switching system 20 (or MSC, standing for the English expression "Mobile

Switching Centre"), a subscriber recording module 50 (or HLR, standing for the English expression "Home Location Register") and an authentication module 52 (or AC, standing for the English expression "Authentication Centre"). The subscriber registration module 50 contains the characteristics identifying each of the subscribers. The authentication module 52 contains the secret key SC of each subscriber, issues the random numbers RN, calculates the cryptographic certificates CC2 and compares the cryptographic certificate CC2 with the cryptographic certificate CC1 calculated by the SIM card.

The part A corresponds to the characteristics of the subscriber to the network and comprises a SIM card 22 which is fitted in the mobile handset 14. The information is exchanged bilaterally between the SIM card 22 and the mobile handset 14 (arrow 24), between the mobile handset 14 and the base station 16 (arrow 26), between the base station 16 and the messaging equipment 18 (arrow 28) and between the message equipment 18 and the network 54 (arrow 30).

In order to authenticate the SIM card and enable a communication, steps (1) to (8) of the method described in the introduction are executed at the initiative of the mobile equipment.

According to the invention, the SIM card 22 and the network 54 are supplemented in order to implement the risk management method. To this end, the SIM card 22 and the network 54 are each supplemented by a so-

called risk management module, referenced 32 for the card and 34 for the server.

The card module 32 contains the matters relating to the subscriber, whilst the network module 34 contains the matters which are necessary to the network 54 for interpreting the information supplied by the card module and making a decision with regard to the authentication to be executed according to certain criteria.

More precisely, the request 36 for authentication of the card by the network 54 by the sending of a random number RN to the card 22 by means of the mobile handset 14 triggers the operations of the module 32 of the card 22. This module analyses this request according to criteria relating to the subscriber and makes a decision according to the steps in the diagram in Figure 2.

Where the module 32 detects a risk, a risk assessment message 38 is transmitted to the network 54 and more particularly to the management module 34, which makes a decision according to the steps in the diagram in Figure 3. This decision or response is transmitted to the card 22 by means of a message 40 which results either in enabling the authentication of the card according to the normal procedure or inhibiting this authentication and more generally blocking the card.

In the diagram in Figure 2, a request (step 70) for authentication of the card by the terminal commences with the transmission to the card of a random

value or random number RN according to the arrow 36 via the handset ME. This authentication request is received by the card (step 72) and processed by the risk management module 32.

This management module 32 comprises principally:

- a state register RMS for indicating the state of the card, blocked or not (RMS being the acronym of the English expression "Risk Management Status"),

- a counter CAC for counting the number N of authentication requests (CAC being the acronym of the English expression "Cumulative Authentication Counter"),

- comparators for comparing the value N of the counter CAC with thresholds T0 and T1 such that T0 < T1.

Where the register RMS is in the inhibited state (step 74), authentication is refused (step 75) so that the management module 32 blocks the card by means of a signal 58.

Where the register RMS is not in the inhibited state, this authentication request increments the counter CAC (step 76) by one unit. The value N resulting from this incrementation is compared (step 78) with the first threshold T0.

If this incremented value is less than T0, the module 32 calculates (step 80) the first cryptographic certificate CC1 (also referred to as a cryptogram) according to the algorithm AL using the random value RA. This certificate CC1 is transmitted (56) to the network 54.

If this incremented value is equal to or greater than T0, it is compared with the second threshold T1 (step 80). If it is equal to or greater than T1, the register RMS is set to the inhibited state (step 82) and authentication is refused according to step 76 so that the management module 32 blocks the card by means of the signal 58.

If the incremented value is less than T1, the management module produces (step 84) a risk assessment request message and transmits it (step 86) to the network 54 according to the arrow 38 in order to be processed therein according to the diagram in Figure 3.

Moreover, as the second threshold T1 is not reached, blocking of the card is not envisaged, so that the card calculates the cryptographic certificate CC1 (step 88) and transmits it (56) to the network 54.

The risk assessment request message 38 is transmitted to the network 54 according to the SMS format and received therein (steps 90 and 92). From this message there are extracted the value N of the counter CAC and the identification number ID of the bearer of the SIM card.

The risk is assessed by means of step 96 according to the value N, the bearer of the card and other specific parameters 102.

If the risk assessment is considered to be high by step 98, the decision is to inhibit use of the card (step 100) by sending an inhibit message 40 to the card.

If the assessment is not considered to be high, the decision is to enable use of the card (step 102) by sending an enable message 40 to the card. This enable message may contain other elements for, for example, resetting the counter CAC or introducing therein a number determined by the network module 34.

The description of the invention which has just been given shows that the fitting of two risk management modules, one 32 in the SIM card and the other 34 in the network, affords flexibility of the risk management, partly by the card by means of parameters which are simple to use (values of an incremented counter and of thresholds T0 and T1) and partly by the network using more sophisticated parameters which may easily be modified.

The above description shows that it is possible to define a method which comprises the following steps in the electronic chip card 22 consisting in:

(a) checking (74) the state, blocked or not, of the electronic chip card in order to refuse (75) or not the authentication request;

(b) in the case of authorisation of the authentication request, counting (76) the number N of requests for authentication of the electronic chip card (22, SIM) by the network (54),

(c) comparing the number N of authentication requests with a first threshold T0,

(d) calculating a cryptographic certificate if N < T0 and transmitting it to the network,

(e) comparing the number N with a second threshold T1 if $N \geq T0$,

(f) putting the electronic chip card (22, SIM) in the blocked state (52, 58) if $N \geq T1$, and

(g) calculating a cryptographic certificate (88) and producing a risk assessment request message (86) and transmitting them (38, 56) to the network if $T0 < N \leq T1$.

The above steps are supplemented in the network by the following steps consisting in:

(h) analysing (54) the risk assessment request message transmitted by the electronic chip card (22),

(i) assessing (96, 102, 98) the risk according to the results of the analysis according to the previous step (h) and specific parameters, and

(j) producing (100, 104, 40) a response message and transmitting it to the electronic chip card (22).

In describing the invention it has been assumed that the cryptographic certificate is calculated from a random number RA but it is clear that this random number can be replaced by a number which is not random.

Moreover, the particular example which has been described relates to the detection of accesses of a fraudulent nature through their high number; however, the invention also applies to the detection of other conditions which would correspond to other types of access which would constitute a risk for the operator of the network such as the exceeding of a credit allocated to the user of a prepayment card. In this case, the thresholds T0 and T1 would be monetary values

whilst the counter would be a totaller for the expenditure made by the user of the handset. Thus T0 would be a threshold of authorised expenditure whilst T1 would be a threshold beyond which the expenditure would no longer be authorised.

CLAIMS

1. A risk management system in a mobile telephony network equipped with a message service device (18), the mobile handsets (14) each having an electronic chip card (22) (SIM) capable of calculating a cryptographic authentication certificate from a value supplied by the network, characterised:

- in that the electronic chip card (22, SIM) comprises means (32) for enabling or not the calculation of a cryptographic certificate and its transmission (56) to the network when certain conditions are fulfilled or not and for transmitting to the network a message (38) requesting evaluation of the risk when other conditions are fulfilled, and

- in that the network (54) comprises means (34) for evaluating the said risk according to the information contained in the risk evaluation request message (38) and parameters specific to the user of the mobile handset (14, ME) and for sending a message (40) to the said means (32) of the electronic chip card for enabling or not the calculation and transmission of the cryptographic certificate.

2. A method for implementing the risk management system according to Claim 1, characterised in that it comprises, in the electronic chip card (22), the following steps consisting in:

(a) checking (74) the state, inhibited or not, of the electronic chip card in order to refuse (75) or not the authentication request;

(b) in the case of authorisation of the authentication request, counting (76) the number (N) of requests for authentication of the electronic chip card (22, SIM) by the network (54),

(c) comparing the number (N) of authentication requests with a first threshold T0,

(d) calculating a cryptographic certificate if $N < T0$ and transmitting it to the network,

(e) comparing the number N with a second threshold T1 if $N \geq T0$,

(f) putting the electronic chip card (22, SIM) in the inhibited state (82, 58) if $N \geq T1$, and

(g) calculating a cryptographic certificate (88) and producing a risk assessment request message (86) and transmitting (38, 56) them to the network if $T0 < N \leq T1$.

3. A method according to Claim 2, characterised in that it also comprises the following steps implemented by the network (54), consisting in:

(h) analysing (94) the risk assessment request transmitted by the electronic chip card (22),

(i) assessing (96, 102, 98) the risk according to the results of the analysis according to the previous step (h) and parameters specific to the user of the mobile handset, and

(j) producing (100, 104, 40) a response message and transmitting it to the electronic chip card (22).

4. A method according to one of the preceding Claims 2 or 3, characterised in that the numbers N, T0 and T1 are monetary values corresponding respectively

to a totalling of the expenditure made in telephone communications, a first authorised expenditure threshold and a second threshold beyond which the expenditure is no longer authorised.

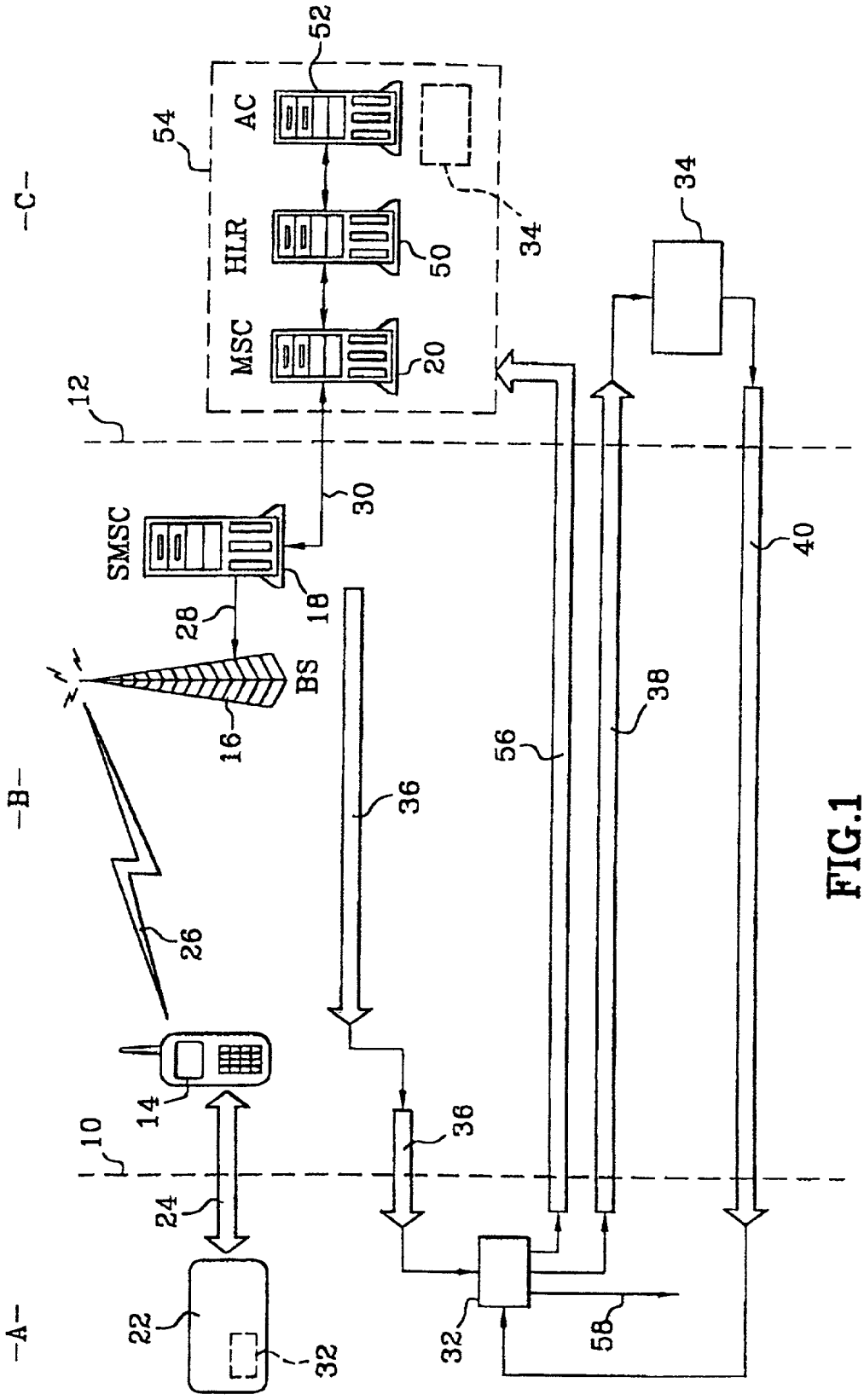
52
54
AC
HLR
MSC
50
20
34
34
12
30
SMSC
18
28
BS
16
36
56
38
40
26
14
10
24
36
22
32
32
58
-A-
-B-
-C-

FIG.1

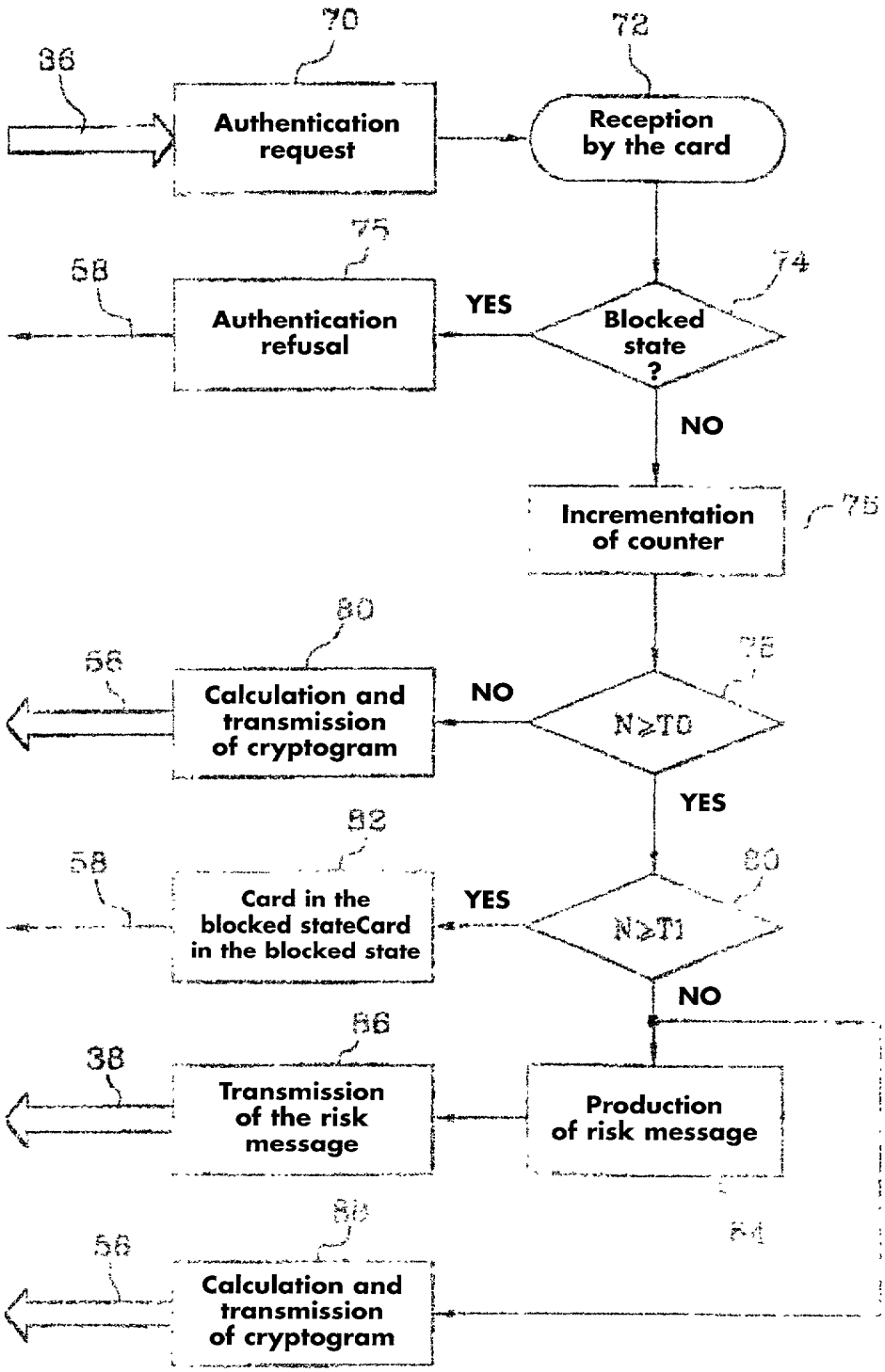

FIG.2

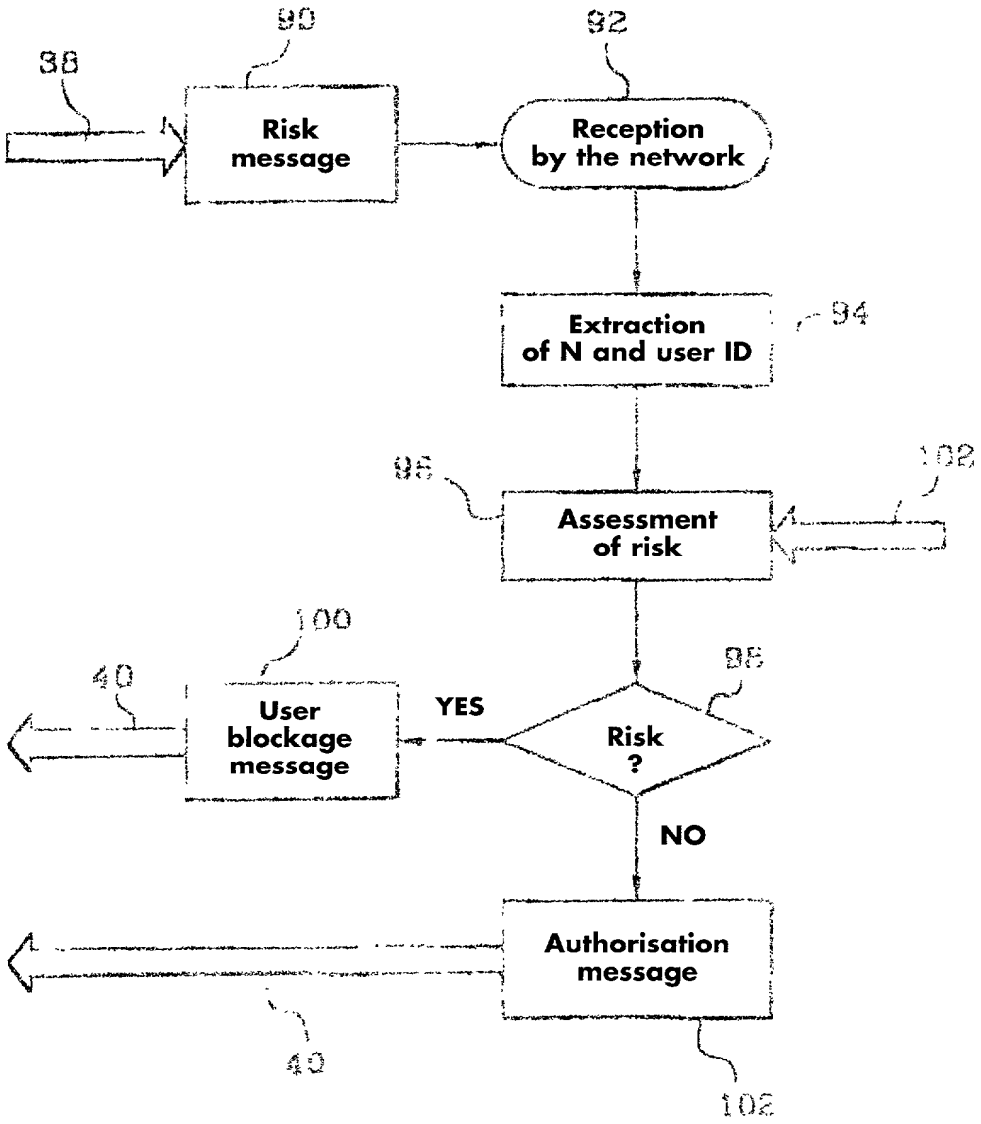

FIG.3

COMBINEDDECLARATIONFORPATENTAPPLICATIONANDPOWEROFATTORNEY (IncludesReferencetoProvisionalandPCTInternationalApplications)	Attorney'sDocketNo.

Asabelownamedinventor,Iherebydeclarethat:
Myresidence,postofficeaddressandcitizenshipareasstatedbelownexttomyname;
IbelieveIamtheoriginal,firstandsoleinventor(ifonlyonenameislistedbelow)oranoriginal,firstandjointinventor (ifpluralnamesarelistedbelow)ofthesubjectmatterwhichisclaimedandforwhichapatentissoughtontheinvention entitled:

MOBILE METHOD AND SYSTEM FOR MANAGING RISK IN A MOBILE TELEPHONE NETWORK.

thespecificationofwhich(checkonlyoneitembelow):

- isattachedhereto
- wasfiledasUnitedStatesapplication
  Number _____
  on _____
  andwasamended
  on _____ (ifapplicable)
- wasfiledasPCTinternationalapplication
  Number PCT/FR99/02233.
  on September 21 1999.
  andwasamended
  on _____ (ifapplicable)

IherebystatethatIhavereviewedandunderstandthecontentsoftheabove-identifiedspecification,includingtheclaims,as amendedbyanyamendmentreferredtoabove.

IacknowledgethedutytodisclosetotheOfficeallinformationknowntometobematerialtopatentabilityasdefinedinTitle 37,CodeofFederalRegulations,§1.56

IherebyclaimforeignprioritybenefitsunderTitle35,UnitedStatesCode,§119(a)-(e)ofanyforeignapplication(s)forpatent orinventor'scertificateorofanyPCTinternationalapplication(s)designatingatleastonecountryotherthantheUnitedStates ofAmericalistedbelowandhavealsoidentifiedbelowanyforeignapplication(s)forpatentorinventor'scertificateoranyPCT internationalapplication(s)designatingatleastonecountryotherthantheUnitedStatesofAmericafiledbymeonthesame subjectmatterhavingafilingdatebeforethatoftheapplication(s)ofwhichpriorityisclaimed:

PRIORFOREIGN/PCTAPPLICATION(S)ANDANYPRIORITYCLAIMSUNDER35U.S.C.§119:

COUNTRY (ifPCT,indicate"PCT")	APPLICATIONNUMBER	DATEOFFILING (day,month,year)	PRIORITYCLAIMED UNDER35U.S.C §119
PCT.	WO 00/25546	4/05/00.	_Yes _No
FRANCE	FR 98 13440	27/10/98	_Yes _No
			_Yes _No
			_Yes _No
			_Yes _No

IherebyclaimthebenefitunderTitle35,UnitedStatesCode§119(e)ofanyUnitedStatesprovisionalapplication(s)listed below.

_____ _____
(ApplicationNumber) (FilingDate)

_____ _____
(ApplicationNumber) (FilingDate)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D) (Includes Reference to Provisional and PCT International Applications)	Attorney's Docket No.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States applications(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose to the Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations §1 56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application

PRIOR U.S APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. §120:

U.S. APPLICATIONS		STATUS *(check one)*		
U.S. APPLICATION NUMBER	U.S FILING DATE	PATENTED	PENDING	ABANDONED
PCT APPLICATIONS DESIGNATING THE U.S.				
PCT APPLICATION NO.	PCT FILING DATE	U.S APPLICATION NUMBERS ASSIGNED (if any)		
PCT/FR99/02233	29.09.99.			

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention

William L Mathis	17,337	R Danny Huntington	27,903	Gerald F Swiss	30,113
Robert S Swecker	19,885	Eric H Weisblatt	30,505	Michael J. Ure	33,089
Platon N Mandros	22,124	James W Peterson	26,057	Charles F Wieland III	33,096
Benton S Duffett, Jr	22,030	Teresa Stanek Rea	30,427	Bruce T Wieder	33,815
Norman H. Stepno	22,716	Robert E. Krebs	25,885	Todd R. Walters	34,040
Ronald L Grudziecki	24,970	William C Rowland	30,888	Ronni S. Jillions	31,979
Frederick G. Michaud, Jr.	26,003	T Gene Dillahunty	25,423	Harold R Brown III	36,341
Alan E. Kopecki	25,813	Patrick C Keane	32,858	Allen R. Baum	36,086
Regis E. Slutter	26,999	Bruce J Boggs, Jr	32,344	Steven M duBois	35,023
Samuel C. Miller, III	27,360	William H Benz	25,952	Brian P O'Shaughnessy	32,747
Robert G Mukai	28,531	Peter K Skiff	31,917	Kenneth B. Leffler	36,075
George A Hovanec, Jr	28,223	Richard J McGrath	29,195	Fred W Hathaway	32,236
James A LaBarre	28,632	Matthew L Schneider	32,814		
E. Joseph Gess	28,510	Michael G Savage	32,596		

21839

and: _____

Address all correspondence to

21839

James A LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L P
P O. Box 1404
Alexandria, Virginia 22313-1404

Address all telephone calls to James A LaBarre at (703) 836-6620

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon

COMBINEDDECLARATIONFORPATENTAPPLICATIONANDPOWEROFATTORNEY(CONT'D)
(IncludesReferencetoProvisionalandPCTInternationalApplications)

Attorney'sDocketNo

100

FULLNAMEOFSOLEORFIRSTINVENTOR LE GALL Jean-Pierre.	SIGNATURE	DATE
RESIDENCE Chemin Saint Marc.		CITIZENSHIP FRANCE.
POSTOFFICEADDRESS Chemin ST Marc FR Le Rousset . 13790		

200

FULLNAMEOFSECONDJOINTINVENTOR,IFANY CHEW GARY.	SIGNATURE	DATE 6/4/2001
RESIDENCE 3400 AV KENT		CITIZENSHIP ~~[illegible]~~ SINGAPORE
POSTOFFICEADDRESS 3400 AV KENT MONTREAL, QUEBEC H3S 1N2 CHK		

FULLNAMEOFTHIRDJOINTINVENTOR,IFANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POSTOFFICEADDRESS		

FULLNAMEOFFOURTHJOINTINVENTOR,IFANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POSTOFFICEADDRESS		

FULLNAMEOFFIFTHJOINTINVENTOR,IFANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POSTOFFICEADDRESS		

FULLNAMEOFSIXTHJOINTINVENTOR,IFANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POSTOFFICEADDRESS		

FULLNAMEOFSEVENTHJOINTINVENTOR,IFANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POSTOFFICEADDRESS		

FULLNAMEOFEIGHTHJOINTINVENTOR,IFANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POSTOFFICEADDRESS		

United States Patent & Trademark Office

Office of Initial Patent Examination -- Scanning Division

Application deficiencies found during scanning:

☐ Page(s)__________ of ______________________________ were not present for scanning. (Document title)

☐ Page(s)__________ of ______________________________ were not present for scanning. (Document title)

☑ ***Scanned copy is best available.*** Drawing.